

National Cyber Alert System

[Archive](#)

Cyber Security Bulletin SB09-251

Vulnerability Summary for the Week of August 31, 2009

The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. The NVD is sponsored by the Department of Homeland Security (DHS) National Cyber Security Division (NCSD) / United States Computer Emergency Readiness Team (US-CERT). For modified or updated entries, please visit the [NVD](#), which contains historical vulnerability information.

The vulnerabilities are based on the [CVE](#) vulnerability naming standard and are organized according to severity, determined by the [Common Vulnerability Scoring System](#) (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of US-CERT analysis.

High Vulnerabilities				
Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- robohelp_server	Unspecified vulnerability in Adobe RoboHelp Server 8 might allow remote attackers to execute arbitrary code via unknown vectors, as demonstrated by the vd_adobe module in VulnDisco Pack Professional 8.7 through 8.11, related to a "remote pre-authentication exploit."	2009-09-04	10.0	CVE-2009-3068 BID MISC MISC MISC SECUNIA MISC MISC
agilewiki -- agilewiki	Unspecified vulnerability in AgileWiki before 0.10.1 has unknown impact and attack vectors related to passwords.	2009-09-01	7.5	CVE-2008-7149 OSVDB CONFIRM
aksoft -- akplayer	Stack-based buffer overflow in akPlayer 1.9.0 allows remote attackers to execute arbitrary code via a long string in a .plt playlist file.	2009-09-03	9.3	CVE-2009-3058 VUPEN MILWoRM SECUNIA MISC
	Multiple SQL injection vulnerabilities in Joker Board (aka JBoard) 2.0 and earlier allow remote	2009-09-		CVE-2009-3059

allpublication -- jboard	attackers to execute arbitrary SQL commands via (1) core/select.php or (2) the city parameter to top_add.inc.php, reachable through sboard.php.	2009-09-03	7.5	3059 VUPEN MISC
alqa6ari -- script_q_r	SQL injection vulnerability in lesson.php in Alqatari Q R Script 1.0 allows remote attackers to execute arbitrary SQL commands via the id parameter. NOTE: some of these details are obtained from third party information.	2009-09-03	7.5	CVE-2009-3061 SECUNIA MISC
artetics -- com_artportal	SQL injection vulnerability in the Artetics.com Art Portal (com_artportal) component 1.0 for Joomla! allows remote attackers to execute arbitrary SQL commands via the portalid parameter to index.php.	2009-09-03	7.5	CVE-2009-3054 XF BID MILWoRM
autonomy -- keyview ibm -- lotus_notes symantec -- brightmail_appliance symantec -- data_loss_prevention_detection_servers symantec -- data_loss_prevention_endpoint_agents symantec -- mail_security symantec -- mail_security_appliance	Buffer overflow in xlssr.dll in the Autonomy KeyView XLS viewer (aka File Viewer for Excel), as used in IBM Lotus Notes 5.x through 8.5.x, Symantec Mail Security, Symantec BrightMail Appliance, Symantec Data Loss Prevention (DLP), and other products, allows remote attackers to execute arbitrary code via a crafted .xls spreadsheet attachment.	2009-09-01	9.3	CVE-2009-3037 VUPEN CONFIRM
bas_bloemsaat -- kingcms	PHP remote file inclusion vulnerability in include/engine/content/elements/menu.php in KingCMS 0.6.0 allows remote attackers to execute arbitrary PHP code via a URL in the CONFIG[AdminPath] parameter.	2009-09-03	7.5	CVE-2009-3056 MILWoRM
coronamatrix -- phpaddressbook	Multiple SQL injection vulnerabilities in index.php in CoronaMatrix phpAddressBook 2.0 allow remote attackers to execute arbitrary SQL commands via the (1) username or (2) parameters.	2009-09-01	7.5	CVE-2008-7145 BID BUGTRAQ OSVDB
debian -- linux	Eval injection vulnerability in scripts/uscan.pl before Rev 1984 in devscripts allows remote attackers to execute arbitrary Perl code via crafted pathnames on distribution servers for upstream source code used in Debian GNU/Linux packages.	2009-09-04	10.0	CVE-2009-2946 DEBIAN CONFIRM CONFIRM CONFIRM
dlecms -- dle	PHP remote file inclusion vulnerability in engine/api/api.class.php in DataLife Engine (DLE) 8.2 allows remote attackers to execute arbitrary PHP code via a URL in the dle_config_api parameter.	2009-09-03	7.5	CVE-2009-3055 BID MILWoRM
docebo -- docebo	SQL injection vulnerability in the autoDetectRegion function in doceboCore/lib/lib.regset.php in Docebo 3.5.0.3 and earlier allows remote attackers to execute arbitrary SQL commands via the Accept-Language HTTP header. NOTE: this can be leveraged to execute arbitrary PHP code using the INTO DUMPFILE command.	2009-09-02	7.5	CVE-2008-7153 CONFIRM
fortinet -- fortigate-1000	Fortinet FortiGuard FortiGate-1000 3.00 build 040075,070111 allows remote attackers to bypass URL filtering via fragmented GET or POST requests that use HTTP/1.0 without the Host header. NOTE: this issue might be related to CVE-2005-3058.	2009-09-04	7.5	CVE-2008-7161 XF BID BUGTRAQ BUGTRAQ

heroshare -- hero_super_player_3000	Buffer overflow in Hero Super Player 3000 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a long filename in a .M3U file. NOTE: this might be related to CVE-2008-4504.	2009-09-04	9.3	CVE-2008-7162 XF BID MISC
htmldc -- htmldoc	Buffer overflow in the set_page_size function in util.cxx in HTMLDOC 1.8.27 and earlier allows context-dependent attackers to execute arbitrary code via a long MEDIA SIZE comment. NOTE: it was later reported that there were additional vectors in htllib.cxx and ps-pdf.cxx using an AFM font file with a long glyph name, but these vectors do not cross privilege boundaries.	2009-09-02	10.0	CVE-2009-3050 MLIST MLIST MLIST CONFIRM SECUNIA MISC CONFIRM
indianpulses -- com_gameserver	SQL injection vulnerability in the Game Server (com_gameserver) component 1.0 for Joomla! allows remote attackers to execute arbitrary SQL commands via the id parameter in a gamepanel action to index.php.	2009-09-03	7.5	CVE-2009-3063 VUPEN BID MILWoRM
jabode -- com_jabode	SQL injection vulnerability in Jabode horoscope extension (com_jabode) for Joomla! allows remote attackers to execute arbitrary SQL commands via the id parameter in a sign task to index.php.	2009-09-08	7.5	CVE-2008-7169 BID MILWoRM
microsoft -- iis	Buffer overflow in the FTP server in Microsoft Internet Information Server (IIS) 5.0 and 6.0 allows remote authenticated users to execute arbitrary code via a crafted NLST command that uses wildcards.	2009-08-31	9.0	CVE-2009-3023 VUPEN BID MILWoRM MILWoRM
numarasoftware -- footprints	Numara FootPrints 7.5a through 7.5a1 and 8.0 through 8.0a allows remote attackers to execute arbitrary commands via shell metacharacters in the (1) transcriptFile parameter to MRegi/MRchat.pl or (2) LOADFILE parameter to MRegi/MRABLoad2.pl. NOTE: some of these details are obtained from third party information.	2009-09-02	10.0	CVE-2008-7158 CONFIRM
ocsinventory-ng -- ocs_inventory_ng	Multiple SQL injection vulnerabilities in Open Computer and Software (OCS) Inventory NG 1.02 for Unix allow remote attackers to execute arbitrary SQL commands via the (1) N, (2) DL, (3) O and (4) V parameters to download.php and the (5) SYSTEMID parameter to group_show.php.	2009-09-01	7.5	CVE-2009-3040 BUGTRAQ CONFIRM MISC
ocsinventory-ng -- ocs_inventory_ng	SQL injection vulnerability in machine.php in Open Computer and Software (OCS) Inventory NG 1.02.1 allows remote attackers to execute arbitrary SQL commands via the systemid parameter, a different vector than CVE-2009-3040.	2009-09-01	7.5	CVE-2009-3042 BUGTRAQ CONFIRM MILWoRM SECUNIA FULLDISC
openoffice -- openoffice.org	Integer underflow in OpenOffice.org (OOo) before 3.1.1 might allow remote attackers to execute arbitrary code via crafted records in the document table of a Word document, leading to a heap-based buffer overflow.	2009-09-02	9.3	CVE-2009-0200 VUPEN BID BUGTRAQ MISC

	Heap-based buffer overflow.			SECUNIA MISC
openoffice -- openoffice.org	Heap-based buffer overflow in OpenOffice.org (OOo) before 3.1.1 might allow remote attackers to execute arbitrary code via unspecified records in a crafted Word document, related to "table parsing."	2009-09-02	9.3	CVE-2009-0201 VUPEN SECTRACK BID BUGTRAQ MISC SECUNIA MISC
phplivesupport. -- phplive!	SQL injection vulnerability in message_box.php in OSI Codes PHP Live! 3.3 allows remote attackers to execute arbitrary SQL commands via the deptid parameter.	2009-09-03	7.5	CVE-2009-3062 MILWORM
phprisk -- netrisk	NetRisk 1.9.7 does not properly restrict access to admin/change_submit.php, which allows remote attackers to change the password of arbitrary users via a direct request.	2009-09-02	7.5	CVE-2008-7155 XF BID MISC
rarlab -- winrar	Multiple unspecified vulnerabilities in RARLAB WinRAR before 3.71 have unknown impact and attack vectors related to crafted (1) ACE, (2) ARJ, (3) BZ2, (4) CAB, (5) GZ, (6) LHA, (7) RAR, (8) TAR, or (9) ZIP files, as demonstrated by the OUSPG PROTOS GENOME test suite for Archive Formats.	2009-09-01	10.0	CVE-2008-7144 VUPEN
rein_velt -- vedit	Directory traversal vulnerability in debugger/debug_php.php in Ve-EDIT 0.1.4 allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the _GET[filename] parameter.	2009-09-03	7.5	CVE-2009-3064 VUPEN MILWORM
rein_velt -- vedit	PHP remote file inclusion vulnerability in editor/edit_htmlarea.php in Ve-EDIT 0.1.4 allows remote attackers to execute arbitrary PHP code via a URL in the highlighter parameter.	2009-09-03	7.5	CVE-2009-3065 VUPEN MILWORM
ryo-oh-ki -- shareaza	Multiple unspecified vulnerabilities in Shareaza before 2.3.1.0 have unknown impact and attack vectors related to "very important security fixes," possibly involving update notifications and a domain that is no longer controlled by the vendor.	2009-09-04	10.0	CVE-2008-7164 CONFIRM
sami_ekblad -- page_manager	Unrestricted file upload vulnerability in upload.php in Page Manager 2006-02-04 allows remote attackers to execute arbitrary code by uploading a file with an executable extension, then accessing it via a direct request to the file in an unspecified directory.	2009-09-08	10.0	CVE-2008-7167 XF VUPEN BID MILWORM
snowhall -- silurus_system	SQL injection vulnerability in wcATEGORY.php in Snow Hall Silurus System 1.0 allows remote attackers to execute arbitrary SQL commands via the ID parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-09-04	7.5	CVE-2009-3082 SECUNIA
	SPIP 1.9 before 1.9.2i and 2.0.x through 2.0.8 does not use proper access control for (1)			CVE-2009-

spip -- spip	ecrire/exec/install.php and (2) ecrire/index.php, which allows remote attackers to conduct unauthorized activities related to installation and backups, as exploited in the wild in August 2009.	2009-09-01	7.5	CVE-2009-3041 MISC
synfig -- synfigstudio	Unspecified vulnerability in Synfig Animation Studio before 0.61.08 allows attackers to execute arbitrary code via a crafted .sif file.	2009-09-01	10.0	CVE-2008-7148 CONFIRM
uiga -- church_portal	SQL injection vulnerability in index.php in Uiga Church Portal allows remote attackers to execute arbitrary SQL commands via the month parameter in a calendar action. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-09-04	7.5	CVE-2009-3081 XF SECUNIA OSVDB
yanick_bourbeau -- lightweight_news_portal	Lightweight news portal (LNP) 1.0b does not properly restrict access to administrator functionality, which allows remote attackers to gain administrator privileges via direct requests to admin.php with the (1) potd_delete, (2) potd, (3) vote_update, (4) vote, or (5) modifynews actions.	2009-09-08	7.5	CVE-2008-7172 XF BID MILWoRM

[Back to top](#)**Medium Vulnerabilities**

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Insecure method vulnerability in the UUSee UUUpgrade ActiveX control (UUUpgrade.ocx 3.0.2.12) allows remote attackers to force the download and overwrite of arbitrary files via crafted arguments to the Update method, as exploited in the wild in June 2009.	2009-09-08	6.4	CVE-2008-7168 XF BID MISC
	Multiple directory traversal vulnerabilities in Facil CMS 0.1RC allow remote attackers to read arbitrary files via a .. (dot dot) in the (1) change_lang parameter to index.php or (2) modload parameter to modules.php.	2009-09-08	5.0	CVE-2008-7176 XF BID MILWoRM
absoluteanime -- prime_quick_style	SQL injection vulnerability in root/includes/prime_quick_style.php in the Prime Quick Style addon before 1.2.3 for phpBB 3 allows remote authenticated users to execute arbitrary SQL commands via the prime_quick_style parameter to ucp.php.	2009-09-03	6.5	CVE-2009-3052 BID MISC MILWoRM MISC SECUNIA
alex_rabe -- nextgen_gallery	Cross-site scripting (XSS) vulnerability in wp-admin/admin.php in NextGEN Gallery 0.96 and earlier plugin for Wordpress allows remote attackers to inject arbitrary web script or HTML via the picture description field in a page edit action.	2009-09-08	4.3	CVE-2008-7175 BUGTRAQ OSVDB
alice -- gate2_plus_wi-fi	Cross-site request forgery in cpo6_wifi_m_nocif.cgi in the administrator panel in TELECOM ITALIA Alice Gate2 Plus Wi-Fi allows remote attackers to hijack the authentication of administrators for requests that disable Wi-Fi encryption via certain values for the wlChannel and wlRadioEnable parameters.	2009-09-04	6.8	CVE-2008-7165 XF BID BUGTRAQ SECUNIA OSVDB
	Multiple cross-site scripting (XSS) vulnerabilities in Joker			

allpublication -- jboard	Board (aka JBoard) 2.0 and earlier allow remote attackers to inject arbitrary web script or HTML via (1) the notice parameter to editform.php, (2) the edit_user_message parameter to core/edit_user_message.php, or (3) the user_title parameter to inc/head.inc.php, reachable through any PHP script.	2009-09-03	4.3	CVE-2009-3060 VUPEN MISC
aom-software -- beex	Multiple cross-site scripting (XSS) vulnerabilities in AOM Software Beex 3 allow remote attackers to inject arbitrary web script or HTML via the navaction parameter to (1) news.php and (2) partneralle.php.	2009-09-03	4.3	CVE-2009-3057 SECUNIA MISC
apple -- safari	Apple Safari 4.0.3 does not properly block javascript: and data: URIs in Refresh headers in HTTP responses, which allows remote attackers to conduct cross-site scripting (XSS) attacks via vectors related to (1) injecting a Refresh header that contains a javascript: URI, (2) entering a javascript: URI when specifying the content of a Refresh header, (3) injecting a Refresh header that contains JavaScript sequences in a data:text/html URI, or (4) entering a data:text/html URI with JavaScript sequences when specifying the content of a Refresh header.	2009-08-31	4.3	CVE-2009-3016 XF MISC
ber_kessels -- refine_by_taxo	Cross-site scripting (XSS) vulnerability in Refine by Taxonomy 5.x before 5.x-0.1, a module for Drupal, allows remote attackers to inject arbitrary web script or HTML via a taxonomy term, which is not properly handled by refine_by_taxo when displaying tags.	2009-09-01	4.3	CVE-2008-7150 CONFIRM CONFIRM
bittorrent -- bittorrent utorrent -- utorrent	Buffer overflow in the web interface in BitTorrent 6.0.1 (build 7859) and earlier, and uTorrent 1.7.6 (build 7859) and earlier, allows remote attackers to cause a denial of service (memory consumption and crash) via a crafted Range header. NOTE: this is probably a different vulnerability than CVE-2008-0071 and CVE-2008-0364.	2009-09-04	5.0	CVE-2008-7166 VUPEN VUPEN SECUNIA SECUNIA OSVDB OSVDB MISC
cpanel -- cpanel	Absolute path traversal vulnerability in the Disk Usage module (frontend/x/diskusage/index.html) in cPanel 11.18.3 allows remote attackers to list arbitrary directories via the showtree parameter.	2009-09-01	5.0	CVE-2008-7142 XF MISC BID BUGTRAQ OSVDB
docebo -- docebo	Docebo 3.5.0.3 and earlier allows remote attackers to obtain sensitive information via a direct request to (1) class/class.conf_fw.php, (2) class.module/class.event_manager.php, (3) lib/lib.domxml5.php, or (4) menu/menu_over.php in doceboCore/; or (5) class/class.conf_cms.php, (6) lib/lib.compose.php, (7) modules/chat/teleskill.php, or (8) class/class.admin_menu_cms.php in doceboCms/; which reveals the installation path in an error message.	2009-09-02	5.0	CVE-2008-7154 MISC
drupal -- drupal drupal -- live	Cross-site request forgery (CSRF) vulnerability in Live 5.x before 5.x-0.1, a module for Drupal, allows remote attackers to hijack the authentication of unspecified privileged users for requests that can be leveraged to execute arbitrary PHP code.	2009-09-01	6.8	CVE-2008-7151 XF CONFIRM CONFIRM
skinboard skinboard	EkinBoard 1.1.0 and earlier, when register_globals is enabled, allows remote attackers to bypass authorization	2009-09-	6.0	CVE-2008-7156 VUPEN

ekinboard -- ekinboard	and gain administrator privileges by setting the _groups[] parameter to 2, as demonstrated via backup.php.	02	0.0	AF BID MILWoRM
ekinboard -- ekinboard	Unrestricted file upload vulnerability in EkinBoard 1.1.0 and earlier allows remote attackers to execute arbitrary code by uploading an avatar file with an executable extension followed by a safe extension, then accessing it via a direct request to the file in uploaded/avatars/.	2009-09-02	6.8	CVE-2008-7157 XF BID MILWoRM
eye.fi -- eye-fi_manager	WS-Proxy in Eye-Fi 1.1.2 allows remote attackers to cause a denial of service (crash) via an empty query string to port 59278 and other unspecified vectors.	2009-09-01	5.0	CVE-2008-7137 XF BID BUGTRAQ MISC SECUNIA OSVDB
eye.fi -- eye-fi_manager	The Manager in Eye-Fi 1.1.2 generates predictable snonce values based on the time of day, which allows remote attackers to bypass authentication and upload arbitrary images by guessing the snonce.	2009-09-01	5.0	CVE-2008-7138 BID BUGTRAQ MISC SECUNIA OSVDB
eye.fi -- eye-fi_manager	Multiple cross-site request forgery (CSRF) vulnerabilities in WS-Proxy in Eye-Fi 1.1.2 allow remote attackers to hijack the authentication of users for requests that modify configuration via a SOAPAction parameter of (1) urn:SetOptions for autostart, (2) urn:SetDesktopSync for file upload, or (3) urn:SetFolderConfig for file download location or modification of authentication credentials; and (4) urn:AddNetwork for adding an arbitrary Service Set Identifier (SSID) to hijack the image upload.	2009-09-01	6.8	CVE-2008-7139 XF BID BUGTRAQ MISC SECUNIA OSVDB
gnome -- gdm	The Red Hat build script for the GNOME Display Manager (GDM) before 2.16.0-56 on Red Hat Enterprise Linux (RHEL) 5 omits TCP Wrapper support, which might allow remote attackers to bypass intended access restrictions via XDMCP connections, a different vulnerability than CVE-2007-5079.	2009-09-04	6.8	CVE-2009-2697 REDHAT CONFIRM BID SECUNIA
google -- chrome	Google Chrome 1.0.154.48 and earlier, 2.0.172.28, 2.0.172.37, and 3.0.193.2 Beta does not properly block data: URIs in Refresh headers in HTTP responses, which allows remote attackers to conduct cross-site scripting (XSS) attacks via vectors related to (1) injecting a Refresh header that contains JavaScript sequences in a data:text/html URI or (2) entering a data:text/html URI with JavaScript sequences when specifying the content of a Refresh header. NOTE: the JavaScript executes outside of the context of the HTTP site.	2009-08-31	4.3	CVE-2009-3011 XF MISC MISC
ikiwiki -- ikiwiki	Incomplete blacklist vulnerability in the teximg plugin in ikiwiki before 3.1415926 and 2.x before 2.53.4 allows context-dependent attackers to read arbitrary files via crafted TeX commands.	2009-08-31	5.0	CVE-2009-2944 VUPEN BID
intralearn -- intralearn	IntraLearn Software IntraLearn 2.1, and possibly other versions before 4.2.3, allows remote attackers to obtain sensitive information via a direct request to (1) Knowledge_Impact_Course.htm, (2) LRN-formatted_Course.htm, or (3) Create_Course.htm in help/1/Instructor/, which reveals the installation path in an	2009-09-01	5.0	CVE-2008-7146 MISC OSVDB OSVDB OSVDB

				OSVDB
		error message.		
intralearn -- intralearn		Multiple cross-site scripting (XSS) vulnerabilities in IntraLearn Software IntraLearn 2.1, and possibly other versions before 4.2.3, allow remote attackers to inject arbitrary web script or HTML via the (1) outline and (2) course parameters to library/description_link.cfm, or the (3) records_to_display and (4) the_start parameters to library/courses_catalog.cfm.	2009-09-01	4.3 CVE-2008-7147 MISC OSVDB OSVDB
itd-inc -- bingo!cms_core		Cross-site request forgery (CSRF) vulnerability in bingo!CMS 1.2 and earlier allows remote attackers to hijack the authentication of other users for requests that modify configuration or change content via unspecified vectors.	2009-08-31	6.8 CVE-2009-3022 XF CONFIRM SECUNIA OSVDB JVNDDB JVN
jvitals -- com_agora		Directory traversal vulnerability in the Agora (com_agora) component 3.0.0b for Joomla! allows remote attackers to include and execute arbitrary local files via directory traversal sequences in the action parameter to the avatars page, reachable through index.php.	2009-09-03	6.8 CVE-2009-3053 XF BID MILWORM
linux -- kernel		The tty_ldisc_hangup function in drivers/char/tty_ldisc.c in the Linux kernel before 2.6.31-rc8 allows local users to cause a denial of service (system crash, sometimes preceded by a NULL pointer dereference) or possibly gain privileges via certain pseudo-terminal I/O activity, as demonstrated by KernelTtyTest.c.	2009-09-02	4.9 CVE-2009-3043 BID
maxthon -- maxthon_browser		Maxthon Browser 3.0.0.145 Alpha with Ultramode does not properly block javascript: and data: URIs in Refresh headers in HTTP responses, which allows remote attackers to conduct cross-site scripting (XSS) attacks via vectors related to (1) injecting a Refresh header that contains a javascript: URI, (2) entering a javascript: URI when specifying the content of a Refresh header, (3) injecting a Refresh header that contains JavaScript sequences in a data:text/html URI, or (4) entering a data:text/html URI with JavaScript sequences when specifying the content of a Refresh header; does not properly block data: URIs in Location headers in HTTP responses, which allows user-assisted remote attackers to conduct cross-site scripting (XSS) attacks via vectors related to (5) injecting a Location header that contains JavaScript sequences in a data:text/html URI or (6) entering a data:text/html URI with JavaScript sequences when specifying the content of a Location header; and does not properly handle javascript: URIs in HTML links within (a) 301 and (b) 302 error documents sent from web servers, which allows user-assisted remote attackers to conduct cross-site scripting (XSS) attacks via vectors related to (7) injecting a Location HTTP response header or (8) specifying the content of a Location HTTP response header.	2009-08-31	4.3 CVE-2009-3018 XF BUGTRAQ MISC
microsoft -- iis		Stack consumption vulnerability in the FTP server in Microsoft Internet Information Server (IIS) 5.0 and 6.0 allows remote authenticated users to cause a denial of service (crash) via a list (ls) -R command containing a wildcard that references a subdirectory, followed by a .. (dot dot).	2009-09-04	4.0 CVE-2009-2521 FULLDISC
		Mozilla Firefox 3.0.13 and earlier, 3.5, 3.6 a1 pre, and 3.7 a1		

mozilla -- firefox mozilla -- mozilla mozilla -- seamonkey	pre; SeaMonkey 1.1.17; and Mozilla 1.7.x and earlier do not properly block data: URIs in Refresh headers in HTTP responses, which allows remote attackers to conduct cross-site scripting (XSS) attacks via vectors related to (1) injecting a Refresh header that contains JavaScript sequences in a data:text/html URI or (2) entering a data:text/html URI with JavaScript sequences when specifying the content of a Refresh header. NOTE: in some product versions, the JavaScript executes outside of the context of the HTTP site.	2009-08-31	4.3	CVE-2009-3010 XF MISC MISC
mozilla -- firefox mozilla -- mozilla mozilla -- seamonkey	Mozilla Firefox 3.0.13 and earlier, 3.5, 3.6 a1 pre, and 3.7 a1 pre; SeaMonkey 1.1.17; and Mozilla 1.7.x and earlier do not properly handle javascript: URIs in HTML links within 302 error documents sent from web servers, which allows user-assisted remote attackers to conduct cross-site scripting (XSS) attacks via vectors related to (1) injecting a Location HTTP response header or (2) specifying the content of a Location HTTP response header.	2009-08-31	4.3	CVE-2009-3014 XF BUGTRAQ MISC MISC
nokia -- inresobject.dll	A certain ActiveX control in Inresobject.dll 7.1.1.119 in the Research In Motion (RIM) Lotus Notes connector for BlackBerry Desktop Manager 5.0.0.11 allows remote attackers to cause a denial of service (Internet Explorer crash) by referencing the control's CLSID in the classid attribute of an OBJECT element.	2009-09-01	5.0	CVE-2009-3038 MILWORM
nokia -- qt	src/network/ssl/qsslcertificate.cpp in Nokia Trolltech Qt 4.x does not properly handle a '\0' character in a domain name in the Subject Alternative Name field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.	2009-09-02	5.0	CVE-2009-2700 VUPEN
opera -- opera_browser	Opera 9.52 and earlier, and 10.00 Beta 3 Build 1699, does not properly block data: URIs in Location headers in HTTP responses, which allows remote attackers to conduct cross-site scripting (XSS) attacks via vectors related to (1) injecting a Location header that contains JavaScript sequences in a data:text/html URI or (2) entering a data:text/html URI with JavaScript sequences when specifying the content of a Location header. NOTE: the JavaScript executes outside of the context of the HTTP site.	2009-08-31	4.3	CVE-2009-3013 XF MISC MISC
opera -- opera	Opera before 10.00 does not properly handle a (1) '\0' character or (2) invalid wildcard character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority.	2009-09-02	5.0	CVE-2009-3044 CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM
opera -- opera_browser	Opera before 10.00 trusts root X.509 certificates signed with the MD2 algorithm, which makes it easier for man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted server certificate.	2009-09-02	5.0	CVE-2009-3045 CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM
				CVE-2009-3046

opera -- opera	Opera before 10.00 does not check all intermediate X.509 certificates for revocation, which makes it easier for remote SSL servers to bypass validation of the certificate chain via a revoked certificate.	2009-09-02	5.0	CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM
opera -- opera_browser	Opera before 10.00, when a collapsed address bar is used, does not properly update the domain name from the previously visited site to the currently visited site, which might allow remote attackers to spoof URLs.	2009-09-02	4.3	CVE-2009-3047 CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM
opera -- opera	Opera before 10.00 on Linux, Solaris, and FreeBSD does not properly implement the "INPUT TYPE=file" functionality, which allows remote attackers to trick a user into uploading an unintended file via vectors involving a "dropped file."	2009-09-02	4.3	CVE-2009-3048 CONFIRM CONFIRM CONFIRM CONFIRM
opera -- opera_browser	Opera before 10.00 does not properly display all characters in Internationalized Domain Names (IDN) in the address bar, which allows remote attackers to spoof URLs and conduct phishing attacks, related to Unicode and Punycode.	2009-09-02	5.0	CVE-2009-3049 CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM
orcabrowser -- orca_browser	Orca Browser 1.2 build 5 does not properly block data: URIs in Refresh and Location headers in HTTP responses, which allows remote attackers to conduct cross-site scripting (XSS) attacks via vectors related to (1) injecting a Refresh header that contains JavaScript sequences in a data:text/html URI, (2) entering a data:text/html URI with JavaScript sequences when specifying the content of a Refresh header, (3) injecting a Location header that contains JavaScript sequences in a data:text/html URI, or (4) entering a data:text/html URI with JavaScript sequences when specifying the content of a Location header; and does not properly handle javascript: URIs in HTML links within 302 error documents sent from web servers, which allows user-assisted remote attackers to conduct cross-site scripting (XSS) attacks via vectors related to (5) injecting a Location HTTP response header or (6) specifying the content of a Location HTTP response header.	2009-08-31	4.3	CVE-2009-3017 XF BUGTRAQ MISC
phpbb -- phpbb	phpBB 2.0.23 includes the session ID in a request to modcp.php when the moderator or administrator closes a thread, which allows remote attackers to hijack the session via a post in the thread containing a URL to a remotely hosted image, which might include the session ID in the Referer header.	2009-09-01	6.4	CVE-2008-7143 BUGTRAQ OSVDB
pidgin -- pidgin	Unspecified vulnerability in Pidgin 2.6.0 allows remote attackers to cause a denial of service (crash) via a link in a Yahoo IM.	2009-08-31	4.3	CVE-2009-3025 CONFIRM
pidgin -- pidgin	protocols/jabber/auth.c in libpurple in Pidgin 2.6.0, and possibly other versions, does not follow the "require TLS/SSL" preference when connecting to older Jabber servers that do not follow the XMPP specification, which	2009-08-31	5.0	CVE-2009-3026

	causes libpurple to connect to the server without the expected encryption and allows remote attackers to sniff sessions.			CONFIRM
propertywatchscript -- property_watch	Multiple cross-site scripting (XSS) vulnerabilities in PropertyWatchScript.com Property Watch 2.0 allow remote attackers to inject arbitrary web script or HTML via the (1) videoid parameter to tools/email.php and (2) redirect parameter to tools/login.php.	2009-09-03	4.3	CVE-2009-3066 SECUNIA MISC
qtweb -- qtweb	QtWeb 3.0 Builds 001 and 003 does not properly block javascript: and data: URIs in Refresh and Location headers in HTTP responses, which allows remote attackers to conduct cross-site scripting (XSS) attacks via vectors related to (1) injecting a Refresh header that contains a javascript: URI, (2) entering a javascript: URI when specifying the content of a Refresh header, (3) injecting a Refresh header that contains JavaScript sequences in a data:text/html URI, (4) entering a data:text/html URI with JavaScript sequences when specifying the content of a Refresh header, (5) injecting a Location header that contains JavaScript sequences in a data:text/html URI, or (6) entering a data:text/html URI with JavaScript sequences when specifying the content of a Location header.	2009-08-31	4.3	CVE-2009-3015 XF MISC
simon_rycroft -- sid	Multiple PHP remote file inclusion vulnerabilities in Specimen Image Database (SID), when register_globals is enabled, allow remote attackers to execute arbitrary PHP code via a URL in the dir parameter to (1) client.php or (2) taxonservice.php.	2009-09-01	6.8	CVE-2008-7152 XF MISC BID
sinecms -- sinecms	Directory traversal vulnerability in mods/Integrated/index.php in SineCMS 2.3.5 and earlier, when register_globals is enabled, allows remote attackers to include and execute arbitrary local files via the sine[config][index_main] parameter.	2009-09-04	6.8	CVE-2008-7163 XF BID MILWoRM SECUNIA OSVDB
thekelleys -- dnsmasq	Heap-based buffer overflow in the tftp_request function in tftp.c in dnsmasq before 2.50, when --enable-tftp is used, might allow remote attackers to execute arbitrary code via a long filename in a TFTP packet, as demonstrated by a read (aka RRQ) request.	2009-09-02	6.8	CVE-2009-2957 BID MISC
thekelleys -- dnsmasq	The tftp_request function in tftp.c in dnsmasq before 2.50, when --enable-tftp is used, allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via a TFTP read (aka RRQ) request with a malformed blksize option.	2009-09-02	6.8	CVE-2009-2958 CONFIRM CONFIRM BID MISC
vmware -- vmware_studio	Directory traversal vulnerability in a support component in the web interface in VMware Studio 2.0 public beta before build 1017-185256 allows remote attackers to upload files to arbitrary locations via unspecified vectors.	2009-09-02	5.0	CVE-2009-2968 XF VUPEN CONFIRM CONFIRM BID BUGTRAQ MLIST
webformatique -- reservation_manager	Cross-site scripting (XSS) vulnerability in index.php in Reservation Manager allows remote attackers to inject arbitrary web script or HTML via the resman_startdate	2009-09-03	4.3	CVE-2009-3067 SECUNIA

	parameter.		MISC
yanick_bourbeau -- lightweight_news_portal	Multiple cross-site scripting (XSS) vulnerabilities in Lightweight news portal (LNP) 1.0b allow remote attackers to inject arbitrary web script or HTML via the (1) photo parameter to show_photo.php, (2) potd parameter to show_potd.php, or (3) the Current question field in a vote action to admin.php.	2009-09-08	4.3 CVE-2008-7171 XF XF BID MILWoRM

[Back to top](#)

There were no low vulnerabilities recorded this week.

Last updated September 08, 2009

 [Print This Document](#)